

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université M'hamed BOUGARA de BOUMERDES



Faculté des Sciences
Département d'Informatique

MEMOIRE DE MAGISTER

Spécialité : Informatique
Option : Spécification de Logiciel et Traitement de l'Information

Présenté par :
M^{elle} Rebiha HADAoui

*UN IDS basé sur un algorithme
inspiré du fonctionnement de colonies
des fourmis*

Encadré par : Mr.K.Tamine *Maître de conférences* à l'université de limoges

Soutenu devant le jury:

Mr. M. Mezghiche

Mr. M.Lallem.

Mr. M. Ahmed necer

Mr. K. Tamine

Professeur à l'université de Boumerdes

Professeur à l'université de Tizi-Ouzou

Professeur à l'université de Bab ezzouar

HDR. à l'université de Limoges

Président

Examineur

Examineur

Rapporteur

Année Universitaire : 2008/2009

CHAPITRE I.

Réseaux et techniques de protection contre les attaques réseaux.

Sommaire :

Partie I. Réseaux

I.1.Introduction	13
I.2. Définition	13
I.3. Objectifs des réseaux.....	13
I.4. Classification des réseaux.....	14
I.4.1. LAN.....	14
I.4.2. MAN.....	14
I.4.3. WAN.....	14
I.5.Fonctionnement des réseaux.....	14
I.5.1. Modèle OSI.....	15
I.5.2. Modèle TCP/IP.....	17

Partie II. Sécurité informatique

II.1.Introduction	19
II.2. Objectifs	19
II.3. Services principaux	19

II.4. Objectifs des hackers.....	20
II.5. Politique des hackers.....	20
II.5.1 reconnaissance du système.....	21
II.5.2. exploitation du système.....	21
II.5.3. préservation d'accès.....	22
II.5.4. effacement des traces.....	22
II.6. Différents types d'attaques.....	22
II.6.1. attaques réseaux.....	22
II.6.2.attaques applicatives.....	24
II.6.3.attaques par déni de service.....	26
II.6.4.attaques virales.....	28
II.7.Outils de sécurité.....	28
II.7.1. cryptographie, signature électronique et certificat.....	28
II.7.2. Mots de passes.....	30
II.7.3. Firewall.....	31
II.7.4. Scanners de vulnérabilités.....	32
II.7.5. Fichiers historiques.....	32
II.7.6. VPN.....	33
II.7.7. pot de miel.....	35
II.7.8. IDS.....	35
Conclusion.....	36

CHAPITRE II.

Système de Détection d’Intrusions

Sommaire :

II.1.Introduction	37
II.2. Système de détection d’intrusions.....	37
II.3. Fichier historique.....	38
II.4. Caractéristiques d’un système de détection d’intrusions.....	39
II.5. Endroit pour un système de détection d’intrusions.....	40
II.6.. Classification des IDS.....	40
II.6.1.méthodes de détection	42
II.6.2.réponses des IDS.....	45
II.6.3.sources de données à analyser.....	46
II.6.4. paradigme de détection.....	49
II.6.5. mode de supervision.....	49
II.7. Méthodes de classification et d’IA pour la détection d’intrusions... ..	49
II.8. IDS actuels.....	54
II.9. Imperfections des IDS.....	54
Conclusion.....	55

CHAPITRE III.

Base d'apprentissage et de test KDD

Sommaire :

III.1. Introduction	59
III.2. Description de la base d'apprentissage et de test KDD	59
III.3. Attaques de la base KDD	60
III.3.1. Déni de service.....	60
III.3.2. Les attaques de type R2L.....	60
III.3.3. Les attaques de type U2R.....	60
III.3.4. Reconnaissance –Probing.....	60
III.4. Attributs	62
Conclusion.....	64

CHAPITRE IV.

Systeme de detection d'intrusions à base de la méthode

AntClass

Sommaire :

Partie I. La description de la méthode de classification non supervisée *AntClass*

IV.1. Introduction	66
IV.2. Ce que font les fourmis réelles.....	66
IV.3. Les fourmis artificielles	70
IV.4. Algorithme <i>AntClass</i>	70
IV.4.1. Principe de fonctionnement	71
IV.4.2. Hybridation avec les centres mobiles.....	79
IV.5. Algorithme <i>des centres mobiles (K-Means)</i>	80

Partie II. Application de la méthode *AntClass* sur la base KDD

IV.6. L'objectif du présent travail	83
IV.7. Structure IDSAC	83

CHAPITRE V.

Implémentation, test et validation de IDSAC

Sommaire :

Partie I: L'implémentation du système de détection d'intrusions IDSAC

V.1. Introduction	96
V.2. Environnement de développement	96
V.3. Machine et système d'exploitation utilisés	96
V.4. Description du logiciel	97
V.4.1. Phase d'apprentissage	97
• V.4.1.1. Filtrage des connexions normales.....	99
• V.4.1.2. Application de l'algorithme AntClass.....	99
• V.4.1.3. Algorithme des centres mobiles (K-Means).....	108
• V.4.1.4. Paramètres utilisés.....	101
V.4.1.4.1. paramètres pour <i>AntClass</i>	101
V.4.1.4.2. paramètres pour <i>les centres mobiles</i>	111
V.4.2. Phase de détection d'anomalies.....	111

Partie II: Test et résultat

V.5. Résultat de <i>IDSAC</i> sur un jeu de test.....	112
Conclusion.....	114